ABSTRACT

The aim of this invention is to propose a method for the authentication of applications both at the time of their downloading as well as at the time of their execution. This aim is reached by an authentication method of at least one application working in a equipment connected by a network to a control server, said equipment being locally connected to a security module, said application is loaded and/or executed by means of an application execution environment of the equipment and uses resources stored in the security module, comprising the following preliminary steps:

- reception by the control server, via the network, of data comprising at least the identifier of the equipment and the identifier of the security module,

- analysis and verification by the control server of said data,

- generation of a cryptogram comprising a digest of the application, data identifying the equipment and the security module and instructions intended for said module,

- transmission of said cryptogram, via the network and the equipment, to the security module,

- verification of the application by comparing the digest extracted from the cryptogram received with a digest determined by the security module,

said method further comprising steps wherein, during the initialization and/or the activation of the application, the security module executes the instructions extracted from the cryptogram and releases, respectively blocks the access to certain resources of said security module according to the result of the verification suited to this application carried out previously.